Cornellia Chambers
LAW. PRACTICE. RECREATE.

"At the end of our lives all we have is attention and time" – Tristan Harris

DECONSTRUCTION OF THE PERSONAL DATA PROTECTION BILL, 2018

Leading global businesses have been proven to be guilty of using technology to hijack our psychological vulnerabilities. Tristan Harris, ex-google design ethicist, now co-founder – center for humane technology says "once you know how to push peoples buttons you can play them like a piano… And this is what exactly product designers do to your mind. They play your psychological vulnerabilities (consciously and unconsciously) against you in the race to grab your attention". That's why they need our personal data – anonymized, de-identified or otherwise. The essence of what Tristan Harris is saying has been confirmed by many Silicon Valley tech leaders such as Chammath Palihapitiya and Sean Parker amongst others. Several articles have reported that young techies in Silicon Valley are weaning themselves of their own products and sending their children to elite Silicon Valley schools where iPhones, iPads and even laptops are not allowed.

Patterns of misuse of personal data have been widely witnessed, discussed and condemned by global technology thought leaders. These leaders are now advocating the ethical use of personal data. You will understand how your vulnerability is being hacked by following these links:

https://www.youtube.com/watch?v=C74amJRp730
https://www.youtube.com/watch?v=d6e1riShmak
https://www.youtube.com/watch?v=D5-X915iKTc
https://www.youtube.com/watch?v=qsUrOmwI82I
https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia
https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3

This is why governments around the world are enacting strict data protection laws. Are we protecting the interests of our people through the Personal Data Protection Bill, 2018. Right now, we don't think so.

This paper is a deconstruction and critical analysis of the Data Protection Bill 2018. Through our observations and suggestions, we have tried to highlight the reasoning behind our views.

The Data Protection Bill is a critical piece of legislation for the future of our country and its people. It is in this spirit, as citizens of the country and data principals, that we have taken the liberty to share our heartfelt thoughts on the scope, core principles, general structural approach and provisions of the Bill. We hope the readers will appreciate and understand our concerns. Any comments on this paper may be shared with us at help@cornelliachambers.com

A. THE PROPOSED INDIAN LAW ON DATA PROTECTION

The need to protect an individual from misuse of her personal data led to worldwide debates on personal data protection regulation which ultimately also culminated in the construction of the Personal Data Protection Bill, 2018 ("*bill/proposed law*") in India.

The key objective of the proposed law as embodied in its preamble is: to balance the need to protect an individual's right over her personal data, and the need to facilitate the growth of the digital economy that is based on the use of data. Its vision is to create a culture based on trust between individuals and digital businesses.

We observed that the proposed law has lost track of the core objective of the exercise. **Instead of recognizing the need to protect a person (data principal) from being targeted through misuse of her personal data,** and building provisions to prohibit such misuse, **the bill focusses only on an abstract right of an individual over her personal data.** This being the most critical point we call upon the authors of the bill to revisit the draft in this light.

Our primary objective is to ensure that our children and people at large do not fall prey to psychological tricks and remain protected from being psychologically manipulated by technology businesses based on their human vulnerabilities. We recognize the goodness in technology but believe in the importance of an ethical digital economy. This can only be achieved through effective and confident regulation of use of personal data.

In this paper, we seek to critically analyze the bill. We hope that our findings will help in further strengthening the proposed law.

B. MAIN CHARACTERS OF THE PERSONAL DATA PROTECTION BILL 2018

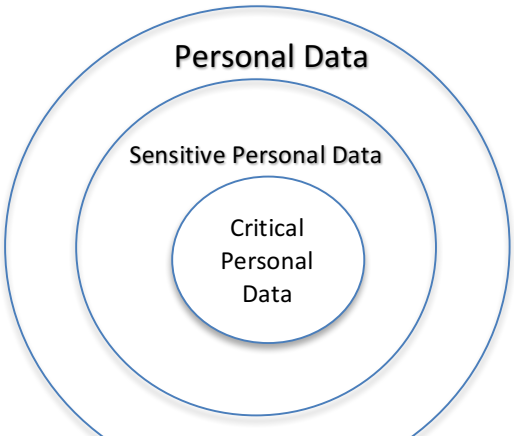
The main characters of this bill are:

Data Principal

A **"data principal"** is an individual present in India whose 'personal data' is being 'processed'.

Categorization of Personal Data under the Bill

There are 3 categories under which 'personal data' has been divided under this proposed law. Personal data, sensitive personal data and critical personal data. Conceptually speaking, sensitive personal data and critical personal data are both subsets of personal data. Critical personal data is a subset of sensitive personal data.



"**Personal data**" has been defined as data of the data principal that can be used to directly or indirectly identify her but does not include anonymized data. '**Anonymized data**' has been defined as data that has been irreversibly transformed into a form in which a data principal cannot be identified (personally)[1]. "**Data**" here would include a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means.

"**Sensitive personal data**" which is a subset of "personal data", has been defined as such data that reveals, is related to, or constitutes (i) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) caste or tribe; and (xii) religious or political belief or affiliation, of a data principal.

Suggestion: We want the government to treat web browsing history and phone numbers as sensitive personal data. Collection of this information should require explicit consent from the data principal.

Data Fiduciary

The proposed law envisages 3 kinds of data fiduciaries (i) data fiduciary (ii) significant data fiduciary and (iii) guardian data fiduciary. Broadly speaking, a significant data fiduciary and a guardian data fiduciary will be a subset of data fiduciaries that will have additional obligations under the proposed law.

"**Data fiduciary**" is a person who alone or together with other persons determines the purpose and means of processing personal data of a data principal. 'Processing' includes operations on personal data - such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination, restriction, erasure or destruction.

"**Significant Data Fiduciary**"[2]: The data protection authority will notify certain data fiduciaries as significant data fiduciaries having regard to factors such as its turnover, volume of personal data processed, sensitivity of personal data processed, risk of harm etc. Data fiduciaries classified as significant data fiduciaries will be required to register with the data protection authority.

"Guardian Data Fiduciary"[3]: The data protection authority is also required to notify data fiduciaries who operate commercial websites or online services directed at children or who process large volumes of personal data of children as 'guardian data fiduciaries'.

Data Processor

[1] This does not restrict identification as part of a community based on factors such as age, gender, location etc.
[2] Section 38
[3] Section 23

The "**data processor**" is a person who processes personal data on behalf of a data fiduciary.

Extra Territorial Applicability of the Data Protection Law on Data Fiduciaries and Data Processors

A data fiduciary or a data processor can be a person/entity that processes personal data of a data principal in connection with:

(i) any goods or services offered to the data principal within the territory of India; or
(ii) any activity which involves profiling (*explained below*) of a data principal within the territory of India. '**Profiling**' here means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interest of a data principal.

A data fiduciary or data processor could be located within India or outside India. They can be an individual, a group of persons or a legal entity of any shape and form – company, trust, society or partnership firms limited or otherwise. Even a government authority could be a data fiduciary.

***Observation**: We note that profiling is used as a tool for persuading a data principal into spending her time and attention on a subject matter. Data fiduciaries have been seen to use profiling consciously to lead the data principals towards specific thoughts and feelings in order to generate the desired behavior from a data principal to serve their commercial interests. More often than not this results in the data principal acting or making decisions that are detrimental to their own interests in an unaware and unconscious state of mind. The problem is bigger than any other problem that we are facing today. Technology product design thinkers around the world have realized the urgency of curbing misuse of personal data for unethical persuasion. In their tech careers, they have had first hand experience of witnessing disastrous effects on populations that were targets of 'unethical persuasion' through "profiling". Having designed these processes/ technological products/ platforms and having witnessed the consequences of such designs closely, they have now become staunch advocates of limiting the use of personal data processing (which results in profiling) only for ethical persuasion. 'Ethical persuasion' has been defined to mean persuasion that is good for the persuasee (i.e. the data principal). We want the government to look into this aspect deeply, because it appears to have been neglected in the proposed law. We strongly believe that one of the core objectives/principles of the bill should be to ensure that personal data is not used for unethical persuasion. This can only be achieved and implemented if heavy penalties including long term imprisonment is prescribed for contravention of the offence of using personal data for unethical persuasion.*

"**Data protection authority**"[4] will be an authority established by the Central Government. As per the proposed law, the functions of the data protection authority, amongst others, will be to ensure compliance with the provisions of the data protection law, to protect the interests of data principals, prevent misuse of personal data, promote awareness of data protection etc.

"**Adjudicating officer**"[5] will be an officer appointed to the adjudication wing of the data protection authority. The broad function of the adjudicating officer will be to adjudicate on complaints/disputes arising out of the data protection law and award compensation & impose penalties (as prescribed in

[4] Chapter X
[5] Section 68.

the data protection law). The adjudicating officer will be a person with specialized knowledge in the fields of constitutional law, cyber and internet laws, information technology law and policy, data protection and related subjects.

"**Arbitral tribunal**" will be established by the Central Government to hear and dispose off any appeal from an order of the Adjudicating officer or the data protection authority.

C. OTHER IMPORTANT CONCEPTS IN THE DATA PROTECTION BILL

"Harm" has been defined to include — (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (iii) financial loss or loss of property; (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal.

Observation: The definition of 'harm' includes 'any observation or surveillance that is not reasonably expected by the data principal'. The authors should specify examples of what they construe as 'unreasonable observation or surveillance'. We appreciate this measure however it will be rendered ineffective and meaningless without examples, especially because there is no jurisprudence in this area as yet.

"**Significant harm**" means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm.

D. PRINCIPALS OF THE BILL

(i) Accountability[8]

Under the proposed law, the data fiduciary is accountable for ensuring compliance with processing related obligations. The bill proposes to hold the data fiduciary accountable, irrespective of whether the processing is undertaken by it, or on its behalf, i.e. through a data processor. The bill also requires a data fiduciary to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of the data protection law.

(ii) Fair and Reasonable Processing[9]

The proposed law seeks to cast an overarching responsibility on the data fiduciaries and the data processors to process personal data in a *'fair and reasonable manner'* that respects the privacy of the data principal.

(iii) Purpose Limitation[10]

[8] Section 11
[9] Section 4
[10] Section 5

Lawful purpose, clear and specific

The proposed law requires the data fiduciary to process personal data only for a lawful purpose. It also requires the data fiduciary to be clear and specific about such a purpose.

Suggestion: In order to protect the interests of data principals, any processing of personal data for unethical persuasion should be expressly prohibited and declared as an 'unlawful purpose' by inserting a specific provision to this effect.

Incidental Purpose[11]

The proposed law also seeks to permit processing of personal data for a purpose 'incidental to the purpose specified to the data principal at the time of collection of her personal data'.

Observation: Our apprehension is that this concept of "incidental purpose" may be misinterpreted and misused. The government should give illustrations that will be indicative of the permitted scope and nature of the intended incidental use.

(iv) Collection[12]

The proposed law requires the data fiduciary to only collect personal data which is necessary for the purposes of processing.

(v) Data Quality[13]

In situations where personal data is likely to be used to make a decision about a data principal, or disclosed to other individuals or entities, or is kept in a form that distinguishes personal data based on facts from personal data based on opinion or personal assessments, the data fiduciary is required to take steps to ensure that the personal data processed is complete, accurate, not misleading and updated in context to the purpose for which it is processed.

Suggestion: To our mind, the implication of this obligation would extend to opinion based platforms such as yourstory.com, Zomato. However, we would suggest that the government should elucidate by example, the kind of platforms that it seeks to cast an obligation of maintaining data quality on.

(vi) Data Storage Limitation[14]

The data fiduciary is required to retain personal data only for as long as it is necessary for the purpose for which it was collected, unless necessary to comply with a legal obligation.

Observation: It is not clear as to whether the exception made would extend to longer periods of storage agreed to in a contract between a data principal and data fiduciary. Further, the proposed law also provides that the personal data must be deleted in a specified manner but does not provide clarity on who will specify the manner of deletion.

---

[11] Section 5 (2)
[12] Section 6
[13] Section 9
[14] Section 10

D. THE HEART OF THE PROPOSED LAW

Observation: The effectiveness of any legislation lies in the clarity with which its provisions set out the rights and obligations of the stakeholders. Lack of clarity in the provisions of a legislation leads to interpretational issues which results in weak implementation of the law. In such situations, the financially stronger stakeholders take undue advantage of the weak implementation and defeat the purpose of the legislation. This ultimately results in continued economic and social disparity where the rich become richer and the poor become poorer (the uneducated and unaware stay subjugated). It is our constitutional imperative to change this by drafting clear laws but the draftsmen of this proposed law have completely failed in fulfilling their duty.

The foundation of data protection laws (around the world) hinges on the concept of notice to the data principal and obtaining an informed consent from the data principal before collection and processing of her data.

Chapter II (Data Protection Obligations), Chapter III (Grounds for Processing of Personal Data) and Chapter IV (Grounds for Processing of Sensitive Personal Data) collectively form the core of this proposed data protection law. These chapters provide for the requirement of giving notice to a data principal and the requirement of obtaining consent from a data principal before collection and/ or processing of her personal data. However, it provides for several exemptions from this core requirement (of obtaining consent) in an unclear manner. The proposed law provides for permutations and combinations of situations where (i) notice and consent are both mandatory, (ii) notice is mandatory but taking of consent is not mandatory, (iii) notice is not mandatory and even consent is not mandatory. It does not provide clarity on where notice and consent is mandatory and where it is not mandatory.

Having broadly identified the overall problem we will now deal with the important provisions made in these chapters specifically and our concerns regarding them.

(i) Notice[15]

The proposed law mandates a data fiduciary to provide the data principal certain prescribed information at the time of collection of the personal data, in the form of a 'notice'. In situations where the personal data is not being collected but only being processed, a data fiduciary is required to give the notice of processing to the data principal as soon as reasonably practical.

Observation: It is not clear as to how data will be processed without being collected. One possible explanation to this provision could be a situation where personal data stored in confidential databases is required to address a medical emergency or situation of natural disaster or break down of public order. If this is the intention, we are of the view that the government should clarify this point preferably using illustrations (such as those found along with provisions in the Indian Contract Act and Indian Penal Code).

Prescribed Information

The proposed law requires that amongst others, the following information should be included in the notice to the data principal: (a) the purposes of processing, (b) categories of personal data being

[15] Section 8

collected, (c) contact details of the data fiduciary, (d) where consent for processing of personal data is mandatory, the process for withdrawal of consent, (**the authors of this bill have not specified where such consent is mandatory and where it is not mandatory**), (e) if the processing of the personal data is based on the grounds mentioned in section 12 to section 22[16] of the proposed law, the data fiduciary is required to provide the basis for such processing and the consequences of the failure to provide such personal data, (f) the source of information, where the personal data is not collected from the data principal, (g) third parties with whom such personal data may be shared, (h) information regarding regarding cross border transfer of personal data, (i) time duration or criteria for retention of data, (j) data principal rights and procedure for their exercise, (k) grievance redressal procedure, (l) data trust score, if any etc.

Suggestion: We want the government to ensure that the 'notice' includes a specific representation from the data fiduciary that any category of personal data will not be used for unethical persuasion and that the data fiduciary understands and agrees that technology tools used for unethical persuasion result in significant harm to a data principal including mental injury. Further, a contravention of this representation and warranty by the data fiduciary, should attract maximum penalty prescribed under the proposed law and the government should have the right to expropriate the investment of a data fiduciary, if it is found guilty of such a contravention. This will ensure that the core objective of the proposed law (i.e., building trust between the digital economy and the data principals) is achieved.

Our thought behind suggesting such strict penalties is that this is the most important legislation of our times. This legislation will help protect the independence of our people's thought process, confidence and will also serve as a fence against any attempts to wage psychological warfare against our nation's security and our people. The use of data to engage in psychological warfare against a nation is being considered and studied as a real threat (to a nation's security) around the world. Defence experts are of the opinion that this is a prevalent practice.

The proposed law also states that the notice should be 'given in multiple languages wherever necessary and practicable'.

Suggestion: It is our suggestion that a data fiduciary should be required to give the notice in at least the two official languages of India i.e. Hindi and English.

Where notice is not required[17]

Section 15 and 21 of the proposed law deals with processing of personal data/ sensitive personal data for prompt action. As per the proposed law, situations requiring prompt action include: responding to any medical emergency involving a threat to life, or health of the data principal, or providing a medical treatment during outbreak of disease; or providing assistance during disaster or breakdown of public order.

---

[16] Section 12 (processing of personal data on the basis of consent), section 13 (processing of personal data for the functions of the state), section 14 (processing of personal data in compliance with law or any order of any court or tribunal), section 15 (processing of personal data necessary for prompt action), section 16 (processing of personal data necessary for purposes related to employment), section 17 (processing of data for reasonable purposes), section 18 (processing of sensitive personal data based on explicit consent), section 19 (processing of sensitive personal data for certain functions of the State), section 20 (processing of sensitive personal data in compliance with law or any order of any court or tribunal), section 21 (processing of certain categories of sensitive personal data for prompt action), section 22 (further categories of sensitive personal data).

[17] Section 15 and 21

In cases where processing of personal data/ sensitive personal data is necessary for prompt action, the proposed law exempts a data fiduciary from the obligation of giving a notice where such a notice would substantially prejudice the purpose (i.e., prompt action) of processing of personal data or sensitive personal data.

Suggestion: *We are of the view that a data fiduciary should be required to serve the notice as soon as reasonably practical in all circumstances. Further, we suggest that to avoid interpretational difficulties, the government should give illustrations of situations where it considers that giving of notice would substantially prejudice the purpose of processing (prompt action) of personal data or sensitive personal data.*

(ii) Consent[18]

General Rule

From a holistic reading of Chapters II, III and IV of the proposed law we are of the view that the general rule advanced by the proposed law that applies to processing of personal data is that, personal data can only be processed (used) by a data fiduciary with the consent of the data principal. Such a consent is required to be taken before the commencement of the processing of any personal data.

Essentials of a valid consent[19]

A consent from a data principal will be considered valid only when it is:

(a) ***free,*** i.e. without coercion, undue influence, fraud, misrepresentation and mistake as to the subject matter of the notice of consent;

(b) ***informed*** correctly through the prescribed notice;

(c) ***specific***, i.e., the giver of consent should be clear about the purpose for which she is giving her consent. This is only possible if the notice for consent is drafted transparently, clearly and with the intention to help the consent giver make a fully informed decision.

In the case of **sensitive personal data** the proposed law requires the data fiduciary to give the data principal the choice of separately consenting to the purposes of, operations in, and the use of different categories of sensitive personal data relevant to processing. [20]

Observations: The bill does not provide any clarity on the expectations around the specific process that a data fiduciary must follow to fulfil the requirement of giving the data principal the choice of separately consenting to the use of their sensitive personal data (as proposed). This provision regarding sensitive personal data will lead to wide spread confusion and misuse.

---

[18] Section 12
[19] Section 12 (2)
[20] Section 18 (2)

(d) ***clear***, i.e., consent given (for processing of personal data) through an affirmative action that is meaningful in a given context. The proposed law also allows for consent to be inferred from the behaviour of a data principal and the circumstances in which such consent is said to be given. For example, when you visit a website where the terms of use and privacy policy is placed at the bottom of the page, the action of continuing to use the website or just making a purchase from it could be construed as affirmative action leading to an assumption of your consent (this is also commonly understood as a browse wrap agreement). The notice for consent would be included in the privacy policy and/ or terms of use.

Unlike in case of personal data, the proposed law provides that, for the processing of sensitive personal data, consent cannot be inferred from conduct in a context. Further, in the case of sensitive personal data, the proposed law requires the data fiduciary (an intermediary/ website owner/ platform) to ***'specifically draw the attention'*** of the data principal to the purpose of processing and operations of processing that may have '***significant consequences***' for the data principal. [21]

Observation: It is not clear what the authors of the bill mean by 'drawing of attention' and 'significant consequences' here. It is absolutely imperative that clear parameters for judging the significance of a consequence be laid down and if that is not possible then such vague and ambiguous terms be removed from the body of such an important legislation.

(e) ***capable of being withdrawn*** by the data principal with ease comparable to which the consent was given.

Burden of Proof of Establishing Consent

The proposed law makes it clear that the data fiduciary shall bear the burden of proof to establish that the consent (of the data principal) is free, informed, specific, clear and capable of being withdrawn with ease.

Withdrawal of consent

The proposed law also makes the data principal responsible for all legal consequences arising out of withdrawal of consent.

Observation: The proposed law does not specify the nature of such 'legal consequences' and we see a problem with this vague, open ended approach. While we also understand that partly the intention behind this proposition is to address situations where the data fiduciary would not be able to provide the product or service for which the personal data was required and that may have cost related implications, however, we also see how this proposition does not take into account withdrawal of consent in situations where the data principal is dissatisfied with the performance of the contract or provision of product or service by the data fiduciary.

Consent – when mandatory & when not mandatory

The proposed law envisages processing of personal data with and without consent. This becomes clear from a reading of Section 8(1)(d) (requirement of notice). However, the difficulty is that the

[21] Section 18 (2)

proposed law has failed to specify clearly the situations where consent of the data principal is mandatory and where it is not mandatory. On a holistic reading of Chapters II, III and IV of the proposed law it may be interpreted that it is the intent of the proposed law to exempt a data fiduciary from the requirement to obtain consent from the data principal for processing her personal data (including sensitive personal data) in the following circumstances:

(i) **Processing of personal data for functions of the state -** where processing of personal data is necessary for any function of the Parliament or any State Legislature, or for the exercise of any function of the state authorized by law, for (a) the provision of any service or benefit to the data principal by the state, or (b) the issuance of any certification, license or permit to a data principal by the state.

(ii) **Processing of personal data in compliance with a law or order or judgment of any court or tribunal in India –** where processing of personal data is (a) explicitly mandated under any law made by the Parliament or State Legislature; or (b) for compliance with any order or judgment of any Court or Tribunal in India.

(iii) **Processing of personal data necessary of prompt action** – where processing is necessary for prompt action i.e. (a) to respond to a medical emergency involving a threat to life or health of a data principal or any other individual; (b) to provide medical treatment to any individual during an epidemic, outbreak of disease or any other threat to public health; and/or (c) to ensure safety of, or provide assistance or services to any individual during any disaster or breakdown of public order.

(iv) **Processing of personal data necessary for employment related purposes such as recruitment/ termination, provision of service/ benefit, attendance verification, performance assessment –** where processing on the basis of consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or taking of consent would involve a disproportionate effort by a data fiduciary due to the nature of processing activities.

(v) **Processing of data for reasonable purposes specified/ notified by the data protection authority –** for any other purposes that the data protection authority may specify in future. Such exemptions will be notified by the data protection authority based on considerations such as public interest, interest of the data fiduciary, impact of processing activity on the rights of the data principal and reasonable expectation of the data principal having regard to the context of processing. When the data protection authority gives an exemption, the authority is required to lay down appropriate safeguards that protect the rights of data principals.

Where necessary, the data protection authority can exempt the data fiduciary from the obligation of giving a notice under Section 8 of the proposed law.

E. Personal and Sensitive Personal Data of Children[22]

The proposed law requires a data fiduciary that processes personal data of children to put in place appropriate mechanisms for age verification and obtaining parental consent. A data fiduciary is required to protect the rights and act in the best interest of children.

[22] Section 25

Guardian Data Fiduciary

The data protection authority is required to notify data fiduciaries who operate commercial websites or online services directed at children or who process large volumes of personal data of children as guardian data fiduciaries.

The proposed law prohibits guardian data fiduciaries from profiling, tracking, monitoring behavior, or directing targeted advertising at children or undertaking any processing that can cause any significant harm to children.

Observation and Suggestion: *We appreciate that the authors of the bill realize the significant harm that activities such as profiling, tracking, monitoring behavior, or directing targeted advertising can cause.*

It is our humble request that the same protection be extended to all other data principals especially because an alarming majority our population (especially in small towns and rural areas) continues to be completely unaware, uneducated and therefore incapable of protecting their own interests. Their psychological vulnerabilities deserve protection just as much as that of children. We would like to once again reiterate that profiling, tracking, monitoring behavior, or directing targeted advertising should as a matter of principle be only permitted for ethical persuasion i.e. persuasion which is in the persuasee's interest – both children and adults.

A data fiduciary that exclusively provides counseling or child protection services will not be required to obtain parental consent. Also, certain additional concessions may be given by the authority to such data fiduciaries in future vis a vis their processing activities.

F. Data Principal Rights

(i) ***Right to confirmation***[23]

The proposed law provides that a data principal can obtain certain information about how her personal data is being used. The data principal can demand from a data fiduciary: (i) a confirmation as to whether her data has been or is being processed; and/ or (ii) a brief summary of her personal data that has been or is being processed; and/ or (iii) a brief summary of the processing activities undertaken in respect to her personal data.

Observations: Keeping in line with the reasons behind this intended legislation we find that in the very least it is important for the data principal whose interest is of paramount importance to have been granted the right to obtain from the data fiduciary, information about the benefits and negative consequences that may result from the processing of her personal data. Globally there has been a debate around the use of personal data in subliminal messaging so as to influence the behaviour of an individual and/ or groups and/ or targeted populations.
It is our understanding that the very core objective of this bill is to ensure that an unaware data principal does not become victim to unethical targeted advertising. Some people also view this technique of subliminal messaging as a form of unethical manipulation of thoughts and behavior of the data principal. The proposed law should keep this in check.

[23] Section 24

(ii) Right to correction[24]

The proposed law also grants the data principal a right to obtain the correction, completion and updation of her personal data. Further, the data fiduciary is required to notify all relevant entities/ individuals to whom such personal data was disclosed regarding such a change in the personal data of an individual particularly where such an action would have an impact on the rights and interests of the data principal or on the decisions made regarding them.

In this regard, the data fiduciary has also been given the right to reject such an application with adequate justification. In a scenario where the data fiduciary rejects the application, the data principal has been granted the right to demand that the data fiduciary indicate along side the relevant personal data, that such personal data is disputed by the data principal. For example, information about a person on wikipedia may be disputed in which case wikipedia may be required to indicate such a dispute.

(iii) Right to Data Portability[25]

The proposed law also gives the data principal the right to receive the following information from the data fiduciary, and request for the transfer of this information to any other data fiduciary:

(i) personal data provided by her to the data fiduciary; or
(ii) personal data generated by the data fiduciary in the course of her use of goods and services;
(iii) personal data which forms part of any profile on the data principal (such as on platforms like Facebook, Amazon, Google, LinkedIn, Zomato etc.) or which the data fiduciary has otherwise obtained.

This right to receive and request for transfer of personal data is referred to as the 'right to data portability'. *Such personal data is required to be shared with the data principal and transferred to another data fiduciary in a structured, commonly used machine-readable format.*

Observation and Suggestion: At present, the proposed law does not set out what such a machine-readable format would be. This could lead to possible future disputes between data fiduciaries and data principals. It is suggested that in order to avoid this, an annexure should be introduced in the proposed law specifying acceptable/ indicative formats in which such information may be provided/ transferred by the data fiduciary.

The right to data portability will be available only where the personal data has been processed through automated means. This right will not be available in cases where the processing is necessary for the functions of the state, compliance of law or where the compliance would reveal a trade secret of any data fiduciary or would not be technically feasible.

Observation: To our mind when the data principal takes the ground of technical infeasibility, it should give satisfactory reasons for the denial of request on this ground otherwise this ground will be misused by data fiduciaries to wriggle out of their responsibility. Hence making this right of the data principal redundant.

(iv) Right to be Forgotten[26]

[24] Section 25
[25] Section 26

The proposed law also grants a data principal the right to restrict or prevent continuing disclosure of her personal data by a data fiduciary (referred to as "*the right to be forgotten*") in the following circumstances:

(i) where it has served the purpose for which it was collected, or
(ii) where the data principal has withdrawn her consent for processing of such personal data, or
(iii) where the processing or disclosure of such personal data is being carried out in contravention of any law.

In order to exercise the right to be forgotten, a data principal is required to file an application before an adjudicating officer. The right to be forgotten will become available only if the adjudicating officer finds that the rights and interests of the data principal in preventing continuing disclosure (of his/her personal data) overrides the right to freedom of speech and expression. The adjudicating officer has been granted the discretion to decide such an application while having regard to factors such as the sensitivity of the personal data, the role of the data principal in public life, the relevance of the personal data in public and the nature of the disclosure and activities of the data fiduciary and the impact on its activities. The detailed procedure for exercising the right has not yet been provided in the proposed law but is expected to be notified as rules subsequently. Further, it may be noted that the adjudicating officer's decision may be subject to review by her again if there is any change in circumstances.

Exercise of Data Principal Rights[27]

Except for the right to be forgotten (where a data principal is required to make an application to the adjudicating officer), all other rights can be exercised by the data principal upon making a request in writing to the data fiduciary. The proposed law gives the data fiduciary the right to charge a reasonable fee for such requests (except in the case of the right to confirmation and access under Section 24 and the right to correction under Section 25 where it is not permitted to charge a fee).

Observation: We noted that the proposed law does not specify a time period for compliance with such a request as yet. Neither does it make setting of such a time period mandatory which we find very odd. It is requested that the government should specify the time period within the principal legislation itself.

Further, the data fiduciary is not obliged to comply with request made by a data principal where in its view such compliance would harm the right of another data principal.

Observation: In this regard, we note that the proposed law does not elucidate situations where compliance would harm the right of another data principal and would recommend that illustrations be provided for clarity.

Further, the proposed law also provides a data principal the right to file a complaint with the data protection authority against a refusal of its request by a data fiduciary. The proposed law allows a data fiduciary to follow its own format to facilitate the exercise of rights by a data principal until the time the law specifies a process for the same.

---

[26] Section 27
[27] Section 28

Observation: These rights will have no meaning until the law prescribes a strict timeline for the data fiduciary for resolution of complaints.

F. TRANSPARENCY AND ACCOUNTABILITY MEASURES – OTHER OBLIGATIONS OF DATA FIDUCIARIES

(i) Privacy by Design[28]

The proposed law requires a data fiduciary to give paramount consideration to a data principal's interest and to embed in its organizational and business functions the principles of the proposed law in spirit and form.

(ii) Transparency[29]

Section 30 of the proposed law also requires a data fiduciary to be transparent in its approach, and to provide easily accessible and clear information to the data principals regarding its personal data processing related practices. The information that a data fiduciary is required to provide to a data principal includes:

(a) categories of personal data collected,
(b) purpose of processing,
(c) rights of a data principal and procedure of exercise,
(d) data trust score (if applicable),
(e) information regarding cross border transfers etc.

Observations: It is not clear as to whether this requirement to share information will be satisfied by giving a notice as set out in section 8 of the proposed law or will this have to be given separately. We observed that majority of the information required to be given under section 30 is also required to be given as a notice under section 8 which will lead to duplication of efforts and will not serve any purpose.

The proposed law also requires a data fiduciary to notify the data principal of important operations involved in the processing of personal data related to the data principal through periodic notifications.

Observation and Suggestion: It is not clear what will be considered as "important operations". Illustrations in this regard will be helpful to avoid difficulties of interpretation.

(iii) Security Standards[30]

The proposed law requires a data fiduciary and data processor to implement "appropriate security safeguards". Depending upon the nature of processing of personal data the proposed law requires, amongst others, use of de-identification and encryption methods.

Observations and Suggestions: One striking difficulty here is that the law around use of encryption technology in India is very unclear and wherever standards of encryption are prescribed such

[28] Section 29
[29] Section 30
[30] Section 31

standards are extremely inadequate in today's digital environment (for example the telecom license agreements prohibit use of bulk encryption (which has not been defined by law), or limits the use of encryption to 40 bit key length in the internet service provider license agreement). Also, as per the provisions of the Information Technology Act 2000, the government was required to prescribe modes and methods of encryption by issuing rules on this subject. These rules have not been notified as yet. The government had released a draft encryption policy in September 2015, which due to widespread criticism was never enforced as law. India urgently needs a robust encryption law which is a prerequisite to the successful implementation of India's data protection law.

It is also important to define appropriate security standards. The International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System - Requirements" is seen as one such internationally accepted security standard. It is widely recognized and the adoption of this standard will help create synergies of work between Indian companies and foreign businesses. It is also recognized by the European Union's General Data Protection Regulations, and is also the prescribed security standard in our current data protection regulation under the Information Technology Act 2000 read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

(iv) **Personal Data Breach**[31]

The proposed law also provides for reporting of data breach by a data fiduciary. It requires a data fiduciary to report a personal data breach to the data protection authority only where, in its own opinion such breach is "*likely to cause harm to any data principal*".

Observations: In effect, this section allows a data fiduciary to stand as a judge in its own cause and to not report data breaches where it considers that harm is not likely to be caused to any data principal.

It is shocking to see that after the reporting of a breach to the data protection authority, the proposed law gives the right to the data protection authority to determine whether or not a breach should be reported to the data principal. In making such a decision the data protection authority is required to take into account the severity of the harm that may be caused to a data principal, or whether some action is required on the part of the data principal to mitigate such harm.

The way that reporting of data breaches is proposed to be handled is completely in derogation to the principles of transparency and accountability that this proposed law set out to advocate. Strangely, the data breach is required to be reported to the data protection authority first and not to the data principal. The concept of harm is intangible and relative to each person. We fail to see how this provision seeks to protect data principals and their interest. In our opinion, this provision is arbitrary and therefore unconstitutional. It should struck out immediately. Our suggestion is that all data fiduciaries and data processors should be put under an obligation to report all data breaches to the data principals and the data protection authority without exception. This will be the key to successful implementation of the data protection law in spirit.

Practically speaking, when a data breach of a prominent data fiduciary occurs it typically impacts thousands or millions of data principals at once. Our question to the authors of this bill is that how do you perceive the data protection authority or the data fiduciary to determine whether or not a small/ severe/ significant breach is going to or is likely to cause "harm" or "significant harm" to a data

[31] Section 32

principal or data principals at large? A data breach may result in causing harm to some data principals and may not cause any harm to any other data principals.

*Also, how does this proposed 'breach reporting mechanism' serve the principle of transparency**? How can the data protection authority decide whether or not a data principal has been harmed or has not been harmed without the data principal being heard? To our mind, this provision has not been drafted keeping in mind the interests of the data principals at all.***

Also, by not making disclosure of data breaches mandatory the proposed law is ensuring that there is no transparency and accountability of data breach incidents as the data principals will have no right in law to seek information regarding breaches from private data fiduciaries. The people of India will be deprived of important data points for research which will be critical for identifying the frequency and magnitude of data breaches, reasons for such data breaches and addressing any negative impact.

Requests for information on such data breaches under the Right to Information Act 2005 are likely to be rejected by the data protection authority and government departments (data fiduciaries) under the garb of exemptions made available under Section 8 of the Right to Information Act 2005.

We want the government to ensure that all data breaches are reported publicly by the data fiduciary and data protection authority on their websites.

(v) ***Data Trust Score***[32]

A data auditor[33] may assign a rating in the form of a data trust score to the data fiduciary based on an audit conducted on such a data fiduciary. The data trust score will be determined basis the criteria that the data protection authority will specify in future.

(vi) **Obligations of Significant Data Fiduciaries**[34]

The proposed law provides that only significant data fiduciaries are required to comply with the following obligations:

(i) conduct data protection impact assessments (S.33),
(ii) keep records (S.34),
(iii) conduct data audits (S. 35) and
(iv) appoint data protection officer (S.36).

The proposed law gives the right to the data protection authority to extend the obligations under these provisions to any other class of data fiduciaries also.

---

[32] Section 35 (5)

[33] As per Section 35(5), the data protection authority can register persons with expertise in the area of information technology, computer systems, data science, data protection or privacy as 'data auditors'. Under the proposed data protection law, a registered data auditor can conduct an audit on a data fiduciary to evaluate its level of compliance with the data protection law and assign a rating to such data fiduciary in the form of a data trust score.

[34] Section 38 (3)

Observation: We don't see the point of excluding (regular) data fiduciaries from the obligation of appointing a data protection officer and keeping records.

The obligations of significant data fiduciaries are discussed in detail below:

(a) Data Protection Impact Assessment[35]

The proposed law provides that where a significant data fiduciary intends to undertake any processing that involves, new technologies, or large scale profiling, or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals; such a data fiduciary will not commence processing unless it has undertaken a data protection impact assessment. The data protection impact assessment is required to include an assessment of potential harm that may be caused to the data principals whose personal data is proposed to be processed.

Observation: The use of the terms 'new technologies' or 'large scale' profiling is vague and ambiguous. It is essential that illustrations be given here and added from time to time.

(b) Record Keeping[36]

The proposed law also provides for record keeping obligations of a significant data fiduciary. The significant data fiduciary is required to maintain records of important operations in the data life cycle, records of review of security safeguards, records of data protection impact assessments and any other records as may be specified by the data protection authority. Such records are required to be maintained in a manner that will be specified by the data protection authority.

(c) Data Audits[37]

The proposed law requires a significant data fiduciary to have its personal data related operations and policies audited annually by an independent data auditor, registered with the data protection authority.

The data protection authority may also order a data fiduciary to conduct an audit in case it is of the view that the data fiduciary is processing personal data in a manner that is likely to cause harm to a data principal.

(d) *Data Protection Officer[38]*

A significant data fiduciary is also required to appoint a data protection officer who will be responsible for providing information and advice to the data fiduciary on issues relating to the proposed law and ensure compliance with the data protection laws. It is clarified that a significant data fiduciary may also assign other functions to a data protection officer.

---

[35] Section 33
[36] Section 34
[37] Section 35
[38] Section 36

Foreign data fiduciaries

Where a significant data fiduciary is not present in India but the proposed law applies to it, such a data fiduciary is also required to appoint a data protection officer who will be based in India and will represent the data fiduciary in its compliance obligations under the proposed law. We appreciate this thought.

(vii) **Grievance Redressal**[39]

Every data fiduciary is required to develop a grievance redressal mechanism for its data principals. A significant data fiduciary is required to appoint a data protection officer and every other data fiduciary is required to appoint an officer for grievance redressal.

Observation and Suggestion: We really think that this distinction is pointless. In our view, all data fiduciaries (including significant data fiduciaries and guardian data fiduciaries) should have a data protection officer who should also take on the function of grievance redressal.

Data fiduciaries are required to resolve grievances within 30 days from the date of receipt of a grievance.

Where the data principal is dissatisfied with the redressal of her grievance she has been given the right to file a complaint before the adjudicating officer. An appeal from the decision of an adjudicating officer can be preferred before the appellate tribunal.

Observation: It appears that as per the proposed law, foreign data fiduciaries dealing with personal data other than sensitive personal data have been exempted from the requirement for appointing a grievance officer and wonder what is the basis of this exemption? The proposed law should expressly mandate that every foreign data fiduciary irrespective of having a presence in India, must appoint a data protection officer that amongst other things will also receive and address grievances.

(viii) Data Processors[40]

The proposed law requires data fiduciaries to enter into a "**valid contract**" with the data processor(s) before engaging a data processor for processing of personal data. Such a data processor is required not to use another data processor without authorization from the relevant data fiduciary, unless the contract between them permits it.

Observations: It is our understanding that as per the Indian Contract Act 1872, a valid agreement is a contract and therefore we request that the phrase 'valid contract' be substituted with the term 'contract', to avoid any interpretational difficulties.

The proposed law also casts an obligation on the data processor, employees of data processor and employees of data fiduciary to process personal data only in accordance with the instructions of the data fiduciary and to keep it confidential.

G. CROSS BORDER TRANSFER OF PERSONAL DATA

[39] Section 39
[40] Section 37

(i) Data Localization[41]

General Rule

In the proposed law, as a general rule, a data fiduciary has been permitted to transfer data outside India. This transfer has been permitted subject to certain terms and conditions which are discussed in the paragraphs below. However, it is pertinent to note that the proposed law requires a data fiduciary to ensure that it stores at least one serving copy of any personal data that it deals with on a server in a data center in India.

Exemptions for Personal Data (not including sensitive personal data and critical personal data) from the General Rule

The proposed law empowers the Central Government to exempt data fiduciaries from storing in India, one serving copy of certain categories of personal data (but not sensitive personal data including critical personal data). Such an exemption may be granted on the grounds of necessity or strategic interests of India. Therefore, the proposed law in effect makes it mandatory for a copy of sensitive personal data including critical personal data to always be stored in India.

Critical personal data

Critical personal data can only be processed in a server in a data center in India. Critical personal data is envisioned as a subset of sensitive personal data and the Central Government will notify the categories of personal data that will constitute critical personal data.

(ii) Cross border transfer[42]

Personal Data and Sensitive Personal Data (excluding critical personal data)

The general rule on transfer of personal data is that it can be transferred outside India subject to the following conditions:

Cross border transfer of personal data (not including sensitive personal data) is permitted where: (a) standard contractual clauses or intra-group schemes have been approved by the data protection authority[43]; *or* (b) the Central Government, after consultation with the data protection authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organization is permissible[44]; ***and*** (c) the data principal has consented to such cross border transfer of personal data;

[41] Section 40
[42] Section 41
[43] A data fiduciary will have reporting obligations with respect to any cross-border transfer that it may make under a contract which adheres to such standard contractual clauses or intra-group schemes. Further, the data fiduciary will bear any liability for the harm caused due to any non-compliance with the standard contractual clauses or intra-group schemes by the transferee.
[44] Central government may permit a transfer to a jurisdiction outside India only where it finds that the relevant personal data will be subject to an adequate level of protection and effectiveness of enforcement by authorities.

Cross border transfer of sensitive personal data (excluding critical personal data) is permitted where: (a) standard contractual clauses or intra-group schemes have been approved by the data protection authority; *or* (b) the Central Government, after consultation with the data protection authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organization is permissible; ***and*** (e) the data principal has explicitly consented to such cross border transfer of sensitive personal data.

Also, with respect to **personal data** including **sensitive personal data (excluding critical personal data),** the data protection authority may approve a particular cross border transfer or set of transfers due to a situation of necessity.

Critical Personal Data

For **cross border transfer of critical personal data:** Critical personal data may be transferred outside India only in the following circumstances:

(a) to a person or entity engaged in providing health or emergency services where such transfer is strictly necessary for prompt action i.e. an action to: (i) respond to a medical emergency involving severe threat to life or health of a data principal and any other individual; (ii) provide medical treatment or health services to any individual during an epidemic or threat to public health; (iii) provide assistance in case public emergency. Such transfers are required to be notified to the data protection authority within the prescribed time period.

(b) to a particular country, a prescribed sector within a country or to a particular international organization that has been prescribed by the Central Government, after consultation with the data protection authority, provided that the transfer is necessary for any class of data fiduciaries or data principals and does not hamper the effective enforcement of the proposed data protection law.

H. EXEMPTIONS

(i) Exemptions for certain purposes

Processing of personal data for the following purposes is exempt from the provisions of the proposed data protection law:

(a) processing of personal data in the interest and security of state;
(b) processing of personal data in the interest of prevention, detection, investigation and prosecution of an offense;
(c) processing of personal data for enforcing any legal right or claim or in relation to any legal proceedings;
(d) processing of personal data by a natural person in the course of a purely personal or domestic purpose[45];
(e) processing of personal data necessary for research, archiving or statistical purposes (subject to a data protection impact assessment required to be undertaken in the prescribed manner);
(f) processing of personal data relevant to a journalistic purpose.[46]

[45] This exemption will not apply where processing involves disclosure to public or is undertaken in connection with any professional or commercial activity.

However, such processing is required to be done in compliance with principles of fair and reasonable processing and appropriate security safeguards as enunciated in the proposed law.

(ii) Exemptions available to small entities processing data through non-automated means

The proposed law grants certain exemptions to small entities processing personal data through non-automated means. A data fiduciary will be considered a small entity in the following circumstances:

(a) if its turnover is not more than 20 lacs rupees or a lower amount that may be prescribed by the central government, in the preceding financial year;
(b) if it does not collect personal data for disclosure to any other individual or entities (including other data fiduciaries or processors); and
(c) if it does not process personal data of more than 100 data principals in any one day in the preceding 12 calendar months.

I. DATA PROTECTION AUTHORITY, ADJUDICATING OFFICERS, APPEALS AND JURISDICTION

(i) Data protection authority[47]

The Central Government will notify the establishment of a data protection authority. It will be the duty of the data protection authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this proposed law, and promote awareness regarding data protection.

Observation and Suggestion: We would like the authors of the proposed law to explain how they perceive promotion of awareness regarding data protection. In our opinion a more pressing concern is to create awareness about the consequences of misuse of personal data for unethical persuasion. We should make our population aware about their psychological vulnerabilities and how they can protect themselves from being targets of manipulation by unethical data fiduciaries and data processors. It should be mandatory for all data fiduciaries and data processors to organize awareness workshops and campaigns for their employees and customers through, amongst other means, their platform and social media. The government should also take out advertisements on national television and popular television and radio channels regarding such issues. Further, the data fiduciaries with a turnover of Rs. 25 crores or more should be required to set aside 1/2 % of their revenue or Rs. 6, 00, 000 (whichever is higher) towards generating awareness (about the consequences of misuse of personal data for unethical persuasion). Data fiduciaries with a turnover of less than 25 crores should be required to deploy at least Rs. 3 lac annually towards generating awareness and such data fiduciaries should be permitted to undertake such awareness activities, independently or collectively with other data fiduciaries.

(ii) Adjudicating Officers[48]

The Central Government will also appoint adjudicating officers for the purpose of imposing penalties and awarding compensation as prescribed under the proposed law.

---

[46] Exemption will apply only where it can be demonstrated that the processing is in compliance with the code of ethic issued by the Press Council of India or any media self-regulatory organization.
[47] Section 49
[48] Section 68

(iii) **Appellate Tribunal**[49]

The Central Government will also establish an appellate tribunal for the purpose of hearing appeals, if any, against orders of adjudicating officers.

(iv) **Appeals to the Supreme Court**[50]

An appeal against an order of the appellate tribunal can be made before the Supreme Court of India.

(iv) **Bar to Jurisdiction of Civil Courts**[51]

The proposed law envisages that civil courts will not have jurisdiction to entertain any matter over which the appellate tribunal has jurisdiction.

Observation: It is not clear as to whether the civil court can take up matters over which the adjudicating officers have jurisdiction, and a clarification on this issue will go a long way is saving the valuable time of the judiciary.

J. PENALTIES AND COMPENSATION

(i) **Penalty**[52]

The proposed law provides for heavy penalties for contravention of its provisions by data fiduciaries. **Penalties may extend up to the tune of Rs. 15 crores, or 4 percent of the total worldwide turnover of the preceding financial year of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary, whichever is higher.** It also provides for specific penalties for the data processors, amongst others, for failing to comply with orders of the data protection authority.

Observations: Drawing inspiration from the European Union's General Data Protection Regulation, we should not under-estimate the importance of protecting our own population from the misuse of their personal data for unethical persuasion by data fiduciaries and data processors. A large part of our population is unaware and uneducated and it is the moral responsibility of the government to play a guardian's role in this context. This is an opportunity for us to protect, preserve and encourage freedom of thought and confidence in our people. Leaders around the world who have led innovation in technology have openly expressed serious concerns around the consequences, that misuse of personal data can have on work efficiencies and the general state of mind of people. Personal data, when misused is capable of being used as a weapon to destroy an entire nation, its capacity and belief system. Our data protection law will define the value system of the tech industry in our country. We must not allow the tech industry to hinge its growth on the basis of tech products that tap into the psychological vulnerabilities of our people and are built to encourage unethical persuasion. This is the moment to define our value systems and expectations clearly as a strong nation and we have no reason to fear – as the world will still include us in their journey of technological evolution, which will take everyone forward together, if done correctly. For this reason, we must not be afraid to set out heavy and strict penalties for contravention of our data protection

[49] Section 79
[50] Section 87
[51] Section 89
[52] Chapter XI

law. This will send a strong message to the world about our seriousness in protecting our people's interest.

Furthermore, we observed that there is no penalty on the data fiduciary for failure to disclose data breach to the data protection authority and to data principals and the proposed law should attract the highest penalties set out under the data protection law.

(ii) Compensation[53]

Under the proposed law, a data principal who has suffered harm due to a violation of the data protection law by a data fiduciary or a data processor, will have the right to seek compensation from the data fiduciary or the data processor. The compensation may be sought by instituting a complaint before the adjudicating officer in the prescribed manner. A complaint may also be instituted collectively by aggrieved data principals.

As per the proposed law, where more than one data fiduciary or data processor are involved in the same processing activity and are found to have caused harm to the data principal, then each data fiduciary or data processor may be ordered to pay the entire compensation to the data principal.

Observations: From a reading of this provision it is not clear as to whether the data fiduciary and data processor, convicted of contravention under the data protection law, will be jointly and/ or severally liable for payment of compensation. A clarification in this regard is necessary to save the valuable time of the judiciary in dealing with interpretational issues in future.

(iii) Recovery of Amounts[54]

The proposed law provides for appointment of recovery officers whose function will be to recover penalty and compensation amounts ordered by adjudicating officers. Such a recovery officer will be empowered to make recoveries through attachment or sale of movable and/or immovable property, attachment of bank accounts, arrest and detention in prison etc. of data fiduciaries and data processors.

Observation: It is not clear as to whether or not the recovery process can be commenced by recovery officers during the pendency of any proceedings before the appellate tribunal and the Supreme Court. It is also not clear as to whether the recovery officer can exercise her powers of recovery, should the matter be finally decided by the appellate tribunal or Supreme Court. A clarification in this regard is extremely important for quick execution of orders and to avoid delay due to interpretational difficulties regarding this provision.

(iv) ***Compensation and penalties under the data protection act vis a vis penalties/compensation under other laws***[55]

The proposed law provides that no compensation awarded or penalty imposed under the data protection law will prevent the award of compensation or imposition of any other penalty or punishment under any law for the time being in force.

---

[53] Section 75
[54] Section 78
[55] Section 76

The proposed law also bars the jurisdiction of civil courts with respect to any matter that is a subject matter of this data protection law.

Observations: It is not clear as to in what circumstances, will an award of compensation or imposition of penalty be attracted under any other law, for a subject matter relating to the data protection law. While we understand that proceedings under the data protection law will not be a bar to criminal proceedings (for eg: proceedings instituted under the Indian Penal Code), however on a reading of the proposed law, it appears that the data protection law envisages a bar on other civil proceedings where the subject matter is one that will be governed by the data protection law. Therefore, a clarification in this regard is needed that will clearly state the circumstances in which an aggrieved data principal can go to a civil court. Such clarification is essential to avoid procedural delays and interpretational difficulties in future.

Offences[56]

Any person who contravenes the proposed law by obtaining, disclosing, transferring or selling personal data which results in significant harm to a data principal may be punished with imprisonment up to 3 years or a fine of Rs. 2 lacs, or both. **"Significant harm"** has been defined as "aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm".

Observation: It is not clear as to how this 'significant harm' will be measured. This definition is very wide and vague and will lead to several interpretational difficulties and delay in proceedings. It will be an impediment to the successful implementation of the data protection law. Illustrations and examples should be provided by the authors that will guide the judiciary in interpreting which situations will be considered as those causing 'significant harm'. This is critical because there is no jurisprudence in this area as yet.

Any person who contravenes the proposed law by obtaining, disclosing, transferring or selling "sensitive personal data" which results in 'harm' to a data principal may be punished with imprisonment of up to 5 years or a fine of Rs. 3 lacs, or both. '**Harm**' has been defined to include bodily or mental injury, theft of identity, financial loss, reputational loss, loss of employment, discriminatory treatment, denial or withdrawal of service etc.

Suggestion: Illustrations for 'mental injury' due to harm and significant harm must be provided in the data protection act, because the jurisprudence around mental injury is at a nascent stage in India.

The proposed law sets out that any person who re-identifies personal data that has been de-identified by the data fiduciary or a data processor or processes such personal data without the consent of the concerned data fiduciary or data processor, will be punishable with imprisonment for a term of up to 3 years or a fine extending to Rs. 2 lacs or both.

Observation: This is a serious offence and highest penalty prescribed under this proposed act must be prescribed. It must be kept in mind that the persons committing this nature of offence will typically be entities/persons that will be highly aware (or will have the resources to educate themselves about the obligations under this data protection law) and financially very sound, and in addition may also be influential. Such paltry penalty will not have a deterrent effect on them. Furthermore, it has been noticed that where imprisonment is only an alternative penalty, it is rarely ever awarded.

[56] Chapter XIII

The proposed law considers the abovementioned offences as cognizable (arrest without warrant) and non-bailable and a police officer not below the rank of an inspector is required to investigate it. From a holistic reading of chapter XIII of the proposed law, it appears that for a contravention of these offenses, a criminal complaint will be filed.

Observation: Clarity is needed on whether the adjudicating officer or appellate tribunal will have the power to decide such matters.

In case an offence is committed by a company or a government department, the person in charge of the conduct of the business of the company and the head of the government, respectively will be proceeded against and punished for the contraventions. The proposed law also states any officer responsible for the decisions that result in contravention of the provisions of the data protection law (even if that officer is not the head or CEO, COO, CTO or any CXO of a data fiduciary or data processor), then that officer will be liable to be penalized under this data protection act.

CONCLUSION:

The debate around protection of personal data is not only about protecting the personal data and privacy of a data principal – the debate and the rage is primarily about the use of data for unethical persuasion practices and the urgent need to protect people from such practices. We want the data protection law of our land to address this problem with courage and conviction. In short, the golden principle of the new data protection law should be to categorically prohibit the use of personal data for unethical persuasion. Ethical persuasion should be understood as anything which is good for the persuasee (data principal).

We note that principally the committee understands our concern as provisions have been built into the Bill to protect children from such unethical practices. Given the level of literacy and unawareness in our country, we strongly believe that it is the government's duty to ensure that its citizens do not become targets of unethical persuasion tactics that are widely used by data fiduciaries and data processors around the world.

****

Note: This paper has been written by Ms. Pritika Kumar and Ms. Ishita Bisht with inputs from Ms. Akshita Goel. The views of the authors are coming from a sense of national pride. All views are personal and are not written to offend any person or entity.